The world is under constant threat from well-planned, sophisticated and coordinated terrorist operations against geographically diverse targets. The train bombings in Madrid, Spain and the killing of Chechen President Akhmad Kadyrov in an explosion at a stadium in the Chechen capital are recent examples that caused significant loss to human life and property.

Figure 1 illustrates the problem. The terrorist networks seek to achieve their goals by destroying valuable targets; they obtain information about the targets from sleeper cells embedded in the target country. Counter-terrorism networks, which include the intelligence agencies, governments, local police and other officials, take preventive and preemptive actions to protect these targets. Intelligence agencies throughout the world are working hard to collect, analyze and interpret intelligence reports and news. According to a recent article, “Decoding the Chatter,” in Time magazine, the analysts at the Terrorist Threat Integration Center in Virginia on an average review 5000 to 6000 pieces of intelligence every day. Currently intelligence analysts are not adequately equipped with information tools to predict a terrorist event out of this vast amount of information. These information tools can empower intelligence agencies with the ability to find pertinent data faster, conduct more efficient and effective analysis, share information with others, relay concerns to the appropriate decision-makers, and support them with better information to make effective decisions.

We suggest a semi-automated model-based tool to detect and track terrorist activity and perform “what if” analyses to gain deeper insights into a potential terrorist activity. We have two probabilistic methods: hidden Markov models (HMMs) and Bayesian networks (BNs). The HMMs detect the monitored terrorist activity and measure local threat levels. BNs combine the likelihoods from many different HMMs to evaluate the cumulative probability of terrorist activity. In other words, the BN represents the overarching terrorist plot and the HMMs, which are related to each BN node, represent detailed terrorist subplots. In this paper, we use them to analyze the threat level of potential terrorist attacks for the 2004 Olympics. The models and scenarios are developed based on information gleaned from open sources.

Choosing model parameters

Predicting a terrorist event out of a vast amount of information is analogous to finding a needle in a haystack. While developing a model of a specific terrorist event out of the available information, one key question is: How much prior information is needed to develop a good model? Or how big does the magnifying lens need to be to find the needle? The correct amount of prior information in the model ensures the right size, magnifying lens.

Another issue that arises is the estimation of the model’s parameters. In this case, a relevant question to ask is: How do we specify the HMM and BN parameters? One approach to obtain the HMM parameters could be using the Baum-Welch algorithm and the maximum-likelihood estimation using historical data. When the historical data is not available, the parameters can be specified according to the model and the state description. For example, if the number of transactions in a state is high, then it is highly probable that the HMM stays in that state for a long time. Similarly, if the transactions related to the state are low, then the probability of remaining in that state is low. Transition probabilities do affect the detection scheme; hence, the probabilities which best fit the scenario should be specified. Another practical requirement is that the model be generic so that it can be easily instantiated for any specific name, place or item related to terrorist activities.

Prior probabilities of BN nodes represent a priori knowledge about the BN model. If historical data is available, then the prior probabilities can be generated using “learning” algorithms; otherwise, they typically would be “best guesses” from intelligence experts. For example, an analyst can specify prior probability in words such as likely, less likely or more likely, and these qualitative assessments can be converted to a range of probability numbers.

Note that the “structure learning” of a BN model is more difficult than “para-
meter learning." In the counter-terrorism domain, it is nearly impossible to get enough training data to learn the model (both topology or parameter). In this article, we assume empirical models can be constructed with the help from experienced intelligence analysts.

**Global threat model**

The global threat model, shown in Fig. 2, is a BN that represents the overall threat from diverse scenarios. The BN represents an intuitive and modular representation of knowledge through causal links among nodes. A BN node represents a random variable, and it has a finite set of states that are mutually exclusive and exhaustive. Each state is associated with a conditional probability of the node, given its parent nodes. The causal links between BN nodes represent direct probabilistic dependencies, and the absence of a link indicates conditional independence. A node is conditionally independent of all its non-descendants given its parents. Probabilities of nodes in BNs are updated whenever new evidence arrives based on Bayes theorem. Let us utilize the following notations:

\[ P (b) \]: Prior probability or belief about a hypothesis \( b \).

\[ P (o | b) \]: Conditional probability of observing \( o \) given hypothesis \( b \) (also called the likelihood function)

\[ P (o) \]: Probability of observing \( o \)

\[ P (b | o) \]: Posterior probability or belief about hypothesis \( b \) after observing \( o \).

Bayes theorem in (1) shows relationship among the above-discussed probabilities:

\[ P (b | o) = \frac{P (o | b) P (b)}{P (o)} \]  \hspace{1cm} (1)

The global threat model is a collection of potential terrorist targets, such as soft targets and sea targets. It also models the circumstances that might lead to an attack. The following steps are involved in building a model for the Olympics:

Choose a set of variables that describes the threat scenario;

Specify the causal relationships among the BN nodes.

Next, potential targets and scenarios are assimilated to predict the global threat.

Sea targets: During the Olympics, cruise ships were used to accommodate nearly 13000 athletes, dignitaries and officials because of the scarcity of hotels. The Port of Piraeus, one of the busiest ports in Europe, was used as an Olympic village. With high security at the Olympic venues, an attack on scale, ports, or shipyards were harder to defend. Greece has a vast coastline of 9320 miles and 6000 islands and islets.

Geographical location: The proximity of Greece to Middle East and Europe could be a tactical advantage for some groups as well.

**Soft targets:** A cluster of nodes in the global threat model represents the terrorist threat on "soft targets." The hotels, casinos, and public transportation were deemed soft targets because they were less secure when compared to the Olympics venues. Terrorist groups might select soft targets to guarantee the greatest effect while exposing them to the least amount of risk.

Delayed construction: The violet colored nodes in the global threat model represent the threat due to delayed construction in Athens. With the construction delays, the security personnel may not have had adequate time to complete assessments of the Olympic venue vulnerabilities, plan for the hardening of potential targets and to restrict access to construction sites.

Miscellaneous: The model also illustrates the ongoing conflict between certain groups that might have caused a terrorist attack in Greece. There was also a remote possibility of a nuclear, chemical or biological attack.

A cluster of nodes in the light sage color indicates the intent of various terrorist organizations. Any one of them could have used the Olympics as a way to carry on the fight for their respective causes.

**Assimilation of threats:** The threats from the discussed scenarios are assimilated into a red colored central node. The numerical results associated with the global threat model can be analyzed by assigning the conditional probabilities in the BN. Each node in the global threat model has a specific HMM associated with it; the HMM predicts the evolution of a specific terrorist activity based on dynamic transaction data.
Evaluating local threats via HMMs

HMMs are especially suited for situations that can be modeled as an underlying (hidden) sequence of states, from which only partial observations of the process are available. Baum and his colleagues developed these theoretical tools in the mid 60s and early 70s. Later, their applicability was popularized through the speech processing community. Since then, a growing number of successful applications have been found almost every field of signal processing. (An excellent tutorial on HMMs is “A tutorial on hidden Markov models and selected applications in speech recognition” by L. Rabiner (Proceedings of the IEEE, vol 2, no. 2, pp 257-286, 1989).)

Briefly, a HMM is a stochastic model used to evaluate the probability of a sequence of events, to determine the most likely state transition path, and to estimate those parameters which produce the best representation of the most likely path.

Mathematically, a discrete HMM is described by three parameters:

\[ \lambda = (A, B, \pi) \]

Here, \( A = \{a_{i,j}, a_{12}, a_{22}, \ldots\} \) represents the transition matrix of the underlying Markov process, \( B = \{b_1, b_2, b_3, \ldots\} \) denotes the probability of emission of a certain symbol from a particular state, and \( \pi \) represents the initial probability distribution of the underlying Markov states.

In this paper, it is assumed that the observed data, which is a series of transactions, is available from an intelligence database. The data represents any kind of travel, task, trust, or communication between any person, place or item of suspicious origin. As more transactions are detected, more links representing the transactions are made in the transaction space. The idea behind using an HMM is that we can represent its underlying states as snapshots of the growing transaction space, as shown in Fig. 3. Note that within each of the states of the HMM is a graphical representation of the terrorist network's activity. By using advanced detection methods employed in multiple-target tracking according to D.B. Reid, and attributed-aided tracking along with standard HMM algorithms, we can detect suspicious activities. This ability lets us develop models for counter-terrorism that are more accurate and effective than is possible with manual methods.

Figure 3 shows the HMM of a hypothetical vehicular (truck) bombing. In Fig. 3, the HMM states are indicated by numbers 1, 2, ..., 9. They are defined from the transactions that are likely to happen during the planning and execution of such an attack. Figure 3 shows the state sequence and the transactions related to the states. The HMM states are explicitly described in the shadowed boxes. The green arrow denotes the actual transaction that defines it, and the black arrow is associated with the previous history of transactions that led to that state.

The HMM corresponds to the steps that might be taken to implement such an attack. This model presents a fictitious group “A” and its affiliated terrorist cell “A1” planning a truck bombing in Athens during the Olympics. The group selects a soft target (away from high security Olympic venues) and performs reconnaissance on it. The high commands in the main group “A,” along with the cell “A1,” recruit terrorists to carry out the bombing. The terrorists are embedded in Greece a few months or a year before the Olympics. The high commands in group “A” send the money via messengers. The terrorist cell “A1” purchases fertilizer-based explosives via terrorist groups in a nearby country. The terrorist cell arranges the vehicle (truck) and prepares the bomb. The terrorist cell holds meetings to discuss the logistics and tactics of the bombing attack. Finally, the terrorists either drive the truck into the target and detonate the bomb or leave the truck near the target.

HMMs detect and track the evolving terrorist activities (in this case, a truck bombing) by continuously evaluating the likelihood of such a terrorist activity, given the observations of the sequence. To detect a single terrorist activity using an HMM involves the forward or forward-backward algorithm; however, in order to continually truck many instantiations of terrorist activity in a cluttered environment, we need to use data association methods. Here we only have suggested an HMM for a truck bombing. But, by adopting a similar approach, HMMs can be developed to represent all the diverse scenarios discussed in the global threat model.

Simulations

An integrated HMM and BN software provides the following types of analysis capabilities to an intelligence analyst:

1) Likelihood of observations: The likelihood of the observations is a quantitative measure of the confidence of the match between the observed events and the template models. The HMM determines whether the monitored activity exists. If the activity is consistent with the models derived in the first step, then it is detected and the related soft evidence is reported to the BNs for further analysis and integration.

HMMs also provide a description of
actors, transaction types, transaction description, transaction time, etc.

2) Probability of a terrorist attack: The BN software uses the soft evidence from the HMMs to produce a belief about the global terrorist threat level. As the real intelligence data is not publicly available, we used synthetically generated data to simulate a terrorist event. The simulated data is a combination of the underlying hidden states of HMM corresponding to the truck bombing that is embedded in the background noise from a benign source. We utilized an abbreviated and simplified model for the global threat model with the states of BN nodes ‘truck bombing attack’ are modeled by the underlying states of the truck bombing HMM. Prior probabilities of BN nodes are specified for all the states.

The likelihood of the observations is shown in Fig. 5 in the form of soft evidence from the truck bombing HMM. For simulation purposes, we speeded up the flow of new transactions to every two seconds. The starting point of HMM is associated with the first time this HMM is detected; thus, we believe with certain probability that the modeled terrorist activity is in progress. A peak probability of 0.75 results when this pattern evolves into the absorbing state of the HMM, and we observe a significant number of transactions for this HMM. This soft evidence is reported to the “truck bombing attack” node. The BN merges all the available information from diverse sources and generates a global alarm, which is shown as the inference of a “central node—terrorist attack” in Fig. 6. Similar trends in BN inference of “central node” and “truck bombing attack” node reflect that BN software updates the belief only when the HMMs detect significant new evidence. The results of this simulation show that the global probability of a terrorist attack peaks around 48%. From the perspective of an analyst, this should be viewed as likely.

False-positives cannot be avoided. But they can be minimized with improved accuracy of the model (by obtaining model parameters and structure from multiple experts) and the accuracy of the sensor data (observations). The model produces “soft” alerts rather than “hard” decisions. It only can be used as one aid to decision making.

Conclusions

Based on an analysis of the current and past terrorist events, probabilistic models can represent the threat of a terrorist attack. Bayesian networks are well-suited for modeling global threats and for computing/assessing the overall threat. The reason is that they fuse information provided by the nodes running HMMs that model the specific terrorist activities. The HMM provides the terrorist activity detection engine with useful information, filtered from a noisy set of data.

The model-based methods suggested here could be utilized by agencies involved in counter-terrorism as templates. Further research includes incorporation of actions of counter-terrorist networks via influence diagrams to obtain a better picture of the real possibility of an attack. By assigning costs to the counter-terrorist actions and to the terrorist threats, optimization techniques can be used to allocate counter-terrorism resources. Another extension that will improve our software is to provide an ability to track multiple terrorist activities simultaneously using multi-target tracking algorithms. The final extension is related to how usable the software is for intelligence analysts.

There are several tools used by intelligence analysts to filter chatter. SEAS is one such tool based on BNs. We cannot compare our tool with other tools because they are based on different methodologies. We need to have consistent metrics defined for such a comparison. Efforts are underway to do just that.

Read more about it

- Genie 2.0, Decision Systems Laboratory, University of Pittsburgh, 2003.

About the authors

Satnam Singh, Haiying Tu, Jeffrey Allanch, and Javier Areta are Electrical and Computer Engineering grad students at the University of Connecticut.

Dr. Peter Willett and Dr. Krishna Pattipati are Professors of Electrical and Computer Engineering at the University of Connecticut.

More information about the authors is available at the following web pages:
Satnam Singh: <http://www.engr.uconn.edu/~sa05013/default.html>
Dr. Krishna Pattipati: <http://www.engr.uconn.edu/cece/cece_facu_pattipati.htm>
Dr. Peter Willett: <http://www.engr.uconn.edu/cece/cece_facu_willett.htm>